AnyConnect-implementatie en prestatie/schaalreferentie voor COVID-19-voorbereiding

Inhoud

Inleiding

Nu landen over de hele wereld de COVID-19-pandemie bestrijden, voeren steeds meer bedrijven op afstand een werkbeleid om de verspreiding van de ziekte te voorkomen. Als resultaat hiervan is er een verhoogde vraag naar Remote Access VPN (RAVPN) om werknemers toegang te bieden tot interne bedrijfsmiddelen. Dit artikel bevat verwijzingen naar configuratiegidsen voor het snel opstellen van RAVPN binnen het netwerk of het identificeren en richten van prestaties of het afstemmen van verwante kwesties.

Uitvoering

Het volgende gedeelte bevat informatie over de configuratie en implementaties van AnyConnect externe toegang op de verschillende Cisco-platforms, evenals informatie over de installatie van certificaten, aangezien de implementatie van het certificaat een integraal onderdeel is van de externe toegang van Cisco vanwege de vereisten voor certificatie voor RAVPN.

Licentie

Licenties zijn vereist om de RAVPN-verbindingen op een apparaat te kunnen beëindigen. ASA-platforms ondersteunen alleen 2 VPN-peers zonder licentie. FTD's zullen niet toestaan dat AnyConnect-configuratie op het apparaat wordt uitgevoerd zonder licentie te geven. Vanwege de COVID-19-uitbraak biedt Cisco gratis tijdelijke licenties om gebruikers te helpen bij het implementeren van RAVPN op hun Cisco-apparaten. Meer informatie hierover is te vinden op: Een NooDCOVID-19 AnyConnect-licentie verkrijgen

AnyConnect-handleidingen voor eerste configuratie

Volg deze snelstartgidsen om AnyConnect Remote Access met de meest gebruikelijke configuraties te implementeren:

- AnyConnect Secure Mobility Client met splitter-tunneling op ASA
- AnyConnect Remote Access VPN-configuratie op FTD
- Initiële AnyConnect-configuratie voor FTD, beheerd door FMC (Video)

Zie hieronder voor de volledige configuratiehandleidingen.

Volledige configuratie-handleidingen

ASA:

- ASA ASDM-configuratie
- ASA CLI-configuratie

FTD:

- FTD beheerd door FDM
- FTD beheerd door FMC

IOS/IOS-XE:

- IOS-router voor SSLVPN
- IOS-XE router voor SSL VPN (alleen CSR)
- IOS/IOS-XE router voor IKEv2 VPN

Installatie-handleidingen voor certificaten

- ASA
- FTD FDM
- FTD FMC
- IOS/IOS-XE

Problemen met prestaties en schalen

Met aanzienlijk verhoogd RAVPN-gebruik kunnen AnyConnect-gebruikers prestatiekwesties ervaren. Zie het volgende om te bepalen hoe deze kwesties moeten worden onderkend en om verzachtingsstrategieën te volgen.

Problemen oplossen en identificatie

Gebruik van hoge CPU's

CPU-gebruik heeft direct invloed op prestaties voor VPN-gebruikers. Het gebruik van CPU's zal toenemen naarmate er meer versleuteld of gedecrypteerd verkeer door het apparaat wordt verwerkt. Het apparaat kan een hoge CPU ervaren wanneer het platform de maximale doorvoersnelheid van VPN nadert die het kan verwerken. Vastgesteld moet worden of het hoge CPU-gebruik het gevolg is van overabonnees op het apparaat of van een ander probleem.

Om te controleren of het apparaat een hoge CPU heeft, wordt gesuggereerd de volgende opdrachten te starten:

procesgebruik zonder nul tonen

cpu - gebruik tonen

Uitvoer van voorbeeld:

```
asa# show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00000000019da592   0x00007fffd808b040     0.0%     0.0%     0.5%   Logger
0x0000000000844596   0x00007fffd807bd60     0.0%     0.0%     0.1%   CP Processing
0x0000000000c0dc8c   0x00007fffd8074960     0.1%     0.1%     0.1%   ARP Thread
   -           -        43.8%    43.8%    40.3%   DATAPATH-0-2209
   -           -        43.9%    43.8%    40.3%   DATAPATH-1-2210

asa# show cpu usage
CPU utilization for 5 seconds = 88%; 1 minute: 88%; 5 minutes: 82%
```

In het bovenstaande voorbeeld wordt opgemerkt dat DATAPATH-0 en DATAPATH-1 87,7% van het totale CPU-gebruik verbruiken. In dit geval, is de ASA oversubscript en is noodzakelijk om te bepalen of dit symptoom door de grote hoeveelheid versleuteld en gedecrypteerd verkeer veroorzaakt is. Dit kan dan worden vergeleken met de VPN-doorvoerwaarde die is gedocumenteerd in het gegevensblad voor dat platform.

Om de totale hoeveelheid VPN-verkeer per seconde te berekenen die door het apparaat gaat, kunnen we de *Input bytes* en *Output bytes* toevoegen binnen het *Global Statistics-*gedeelte dat in de *opdracht Show crypto accelerator statistics* wordt *gevonden*. Op een ASA of FTD, ontgrendel de *encryptie-versnellersstatistieken van de* uitvoershow*,* met de opdracht *duidelijke crypto-versnellersstatistieken*. Wacht een bepaalde tijd en voer vervolgens de opdracht uit: *gegevens over cryptoversnellers*, zoals hieronder aangegeven:

```
asa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
```

```
   Max accelerators: 2
   Max crypto throughput: 1000 Mbps
   Max crypto connections: 5000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 257353
   Input bytes: 271730225                          <----------------
   Output packets: 2740
   Output error packets: 0
   Output bytes: 57793                             <----------------
[…]
```

Neem een paar momentopnamen met specifieke intervallen en haal een gemiddelde doorvoersnelheid in bytes die in bits per seconde (bps) kan worden geconverteerd. De formule om dit te doen is:

$$\frac{[InputBytes + OutputBytes] * 8}{1,000,000 * seconds} = Mbps$$

In het vorige voorbeeld wordt een ***duidelijk*** bevel van de ***crypto versnellator statistiek*** gegeven op tijd 0 seconden. 10 seconden later, werd de opdracht ***show crypto versnellator statistics*** gegeven om de totale bytes over het 10 tweede interval te krijgen. Deze waarden worden dan gebruikt om een bps van 217 Mbps te berekenen die over een 10 seconden interval werd verwerkt. Er kunnen meerdere momentopnamen nodig zijn om een nauwkeuriger gemiddelde te behalen.

Let op dat deze waarden voor al het gecodeerde/gedecrypteerde verkeer (HTTPS, SSL, IPsec, SSH, enz.) zullen toenemen. We kunnen deze waarde gebruiken om de gemiddelde VPN-doorvoersnelheid te bepalen en deze te vergelijken met het gegevensblad. Als de gemiddelde doorvoersnelheid ongeveer de zelfde hoeveelheid is als wat op het gegevensblad voor het platform wordt gezien, wordt het apparaat oversubscript door versleuteld en gedecrypteerd verkeer.

Bovendien kan deze methode niet worden gebruikt om de doorvoersnelheid van VPN op FirePOWER 2100 platforms te bepalen aangezien de tellers niet voor VPN-verkeer verhogen. Dit wordt gevolgd in CSCvt46830 .

Maximum aantal VPN-verbindingen

Wanneer ze het maximale aantal VPN-verbindingen inslaan, kunnen gebruikers perioden van verstoring ervaren waar ze geen verbinding kunnen maken. Wanneer u de AnyConnect Plus- of Apex-licentie activeert, wordt het maximale aantal VPN-peers ontgrendeld. Als dit maximum wordt bereikt, zijn er geen extra gebruikers op het apparaat toegestaan.

Om de maximale hoeveelheid VPN-verbindingen op het apparaat te controleren, controleert u de uitvoer van ***show vpn-sessiondb***:

```
asa# show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client            :     10 :        218 :          11 :        0
  SSL/TLS/DTLS               :     10 :        218 :          11 :        0
```

```
Clientless VPN               :      0 :         73 :           4
  Browser                    :      0 :         73 :           4
-------------------------------------------------------------------------
Total Active and Inactive    :     10             Total Cumulative :    291
Device Total VPN Capacity    :    250
Device Load                  :     4%
-------------------------------------------------------------------------

-------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------
Clientless                   :      0 :         73 :               4
AnyConnect-Parent            :     10 :        218 :              11
SSL-Tunnel                   :     10 :         77 :              10
DTLS-Tunnel                  :     10 :         65 :              10
-------------------------------------------------------------------------
Totals                       :     30 :        433
-------------------------------------------------------------------------
```

Om de totale ondersteunde hoeveelheid gebruikers te bepalen die door het platform wordt ondersteund, controleert u het informatieblad voor uw apparaat hieronder.

Als VPN-gebruikers niet in staat zijn verbinding te maken en u hebt geverifieerd dat het apparaat het maximale aantal VPN-gebruikers niet heeft bereikt, kunt u aanvullende assistentie zoeken bij TAC.

Referenties van gegevensbladen

De volgende datasets markeren zowel het maximale aantal VPN-gebruikers dat door een platform wordt ondersteund als de maximale VPN-doorvoersnelheid op basis van testen. IKEv2 en DTLS AnyConnect zullen naar verwachting een vergelijkbare totale (geaggregeerde) doorvoersnelheid hebben als de IPsec VPN-doorvoersnelheid die in elke sectie wordt vermeld.

- ASAv
- ASA 5500
- ASA 5585
- Firepower 1000
- Firepower 2100
- Firepower 4100
- FirePOWER 9300

Potentiële beperkingen

Split-tunneling mogelijk maken

Standaard zal het groepsbeleid op de ASA en FTD een tunnelverbinding implementeren. Hierdoor wordt al het verkeer dat door RA-klanten over de VPN wordt gegenereerd, verwerkt door het head-end. Aangezien pakketencryptie en decryptie rechtstreeks met het gebruik van CPU's verband houden, is het belangrijk om ervoor te zorgen dat alleen het benodigde verkeer door het VPN-head-end wordt verwerkt zoals toegestaan door het beveiligingsbeleid van het bedrijf. Overweeg het gebruik van een gesplitst tunnelbeleid in plaats van volledige tunnel om het VPN-uiteinde van onnodige lading te redden.

- ASA Split-tunneling
- FTD (FMC) Split Tunneling-gids

Opmerking: Tunnel voert een voor het hele bedrijf geldend parameter beveiligingsbeleid uit terwijl gesplitste tunneling afhankelijk is van het clientapparaat om het internetverkeer van de gebruiker te beschermen. Cisco biedt extra security tools zoals Umbrella om VPN-gebruikers te beschermen wanneer er een gesplitste tunnelbeleid wordt gebruikt.

VPN-taakverdeling implementeren (alleen ASA)

VPN-taakverdeling is een functie die wordt ondersteund op ASA-platforms die twee of meer ASA's de mogelijkheid bieden om VPN-sessiebelasting te delen. Als beide apparaten 500 VPN-peers ondersteunen, door de taakverdeling van VPN tussen hen te configureren, zullen de apparaten in totaal 1000 VPN-peers tussen hen ondersteunen. Deze optie kan worden gebruikt om de hoeveelheid gelijktijdige VPN-gebruikers te verhogen tot boven het tijdstip waarop één apparaat kan worden verwerkt. Klik hier voor meer informatie over VPN-taakverdeling, inclusief het taakverdeling-algoritme: VPN-taakverdeling

Optimalisatie configuratie

Aanvullende services die op het platform zijn ingeschakeld, verhogen de hoeveelheid verwerking en lading op het apparaat. Bijvoorbeeld IPS, SSL decryptie, NAT, enz. Overweeg het configureren van het apparaat als een VPN-concentrator die alleen VPN-sessies beëindigt.

Tunnelprotocol-selectie

Standaard is het groepsbeleid voor ASA's ingesteld op het maken van een DTLS-tunnel. Als UDP 443-verkeer wordt geblokkeerd tussen de VPN-kop en de AnyConnect-client, wordt de client automatisch teruggezet op TLS. Het wordt aanbevolen om DTLS of IKEv2 te gebruiken om de maximale VPN-doorvoerprestaties te verhogen. DTLS biedt betere prestaties dan TLS door minder protocoloverhead. IKEv2 biedt ook een betere doorvoersnelheid dan TLS. Bovendien kan het gebruik van AES-GCM-telefoons de prestaties licht verbeteren. Deze ciphers zijn beschikbaar in TLS 1.2, DTLS 1.2 en IKEv2.

Afdwingen per tunnel QoS (alleen FTD)

QoS kan worden geïmplementeerd om de hoeveelheid verkeer te beperken die naar AnyConnect-gebruikers in de uitgaande richting wordt verzonden. Door dit te doen, kan het VPN head-end elke externe toegangsclient afdwingen om zijn eerlijke deel van grotere bandbreedte te krijgen. Meer informatie over dit onderwerp is te vinden op: FTD-configuratie

Uitvoeren van Crypto Engine Accelerator Bias (alleen ASA)

Crypto Engine Accelerator Bias wordt gebruikt om de crypto cores opnieuw toe te wijzen om het ene encryptie-protocol te prefereren boven het andere (SSL of IPsec). Het doel van deze functie is het optimaliseren van de doorvoersnelheid van AnyConnect als de meerderheid van VPN-tunnels IPsec of SSL gebruikt. Het uitvoeren van deze opdracht kan leiden tot onderbreking van de service en daarom is een onderhoudsvenster vereist. Bovendien kan de verbetering (AnyConnect-doorvoersnelheid en CPU-gebruik) afhankelijk van het verkeersprofiel verschillen. Als het VPN-head-end alleen SSL-sessies of alleen IPsec-sessies beëindigt, kan deze opdracht worden overwogen voor een verdere optimalisatie van het VPN-head-end. U vindt hier de opdracht:

Opdrachtreferenties

Om de huidige crypto kern toewijzing te bekijken, voer de opdracht ***uit om crypto versneller belasting op te versnellen***. Deze opdracht geeft niet de totale hoeveelheid crypto gebruik die het apparaat kan verwerken - de verhouding tussen ssl of ipsec verkeer wordt toegewezen aan elke kern. Om de benaderde hoeveelheid gebruik op het apparaat te vinden, raadpleegt u het bovenstaande gedeelte over het **gebruik** van **hoge CPU** en vergelijkt u de berekende waarde met de waarde in het gegevensblad voor het platform.

Op een ASA-platform dat meestal SSLVPN op externe toegang beëindigt, wordt aanbevolen de crypto kerntoewijzing aan te passen om SSL met de commando ***crypto-motor versnellerkaart-bias ssl*** te begunstigen.

Het volgende voorbeeld toont de kerntoewijzing op een ASA5555 met de ***crypto-motor versneller-bias ssl opdracht*** om AnyConnect SSL-klanten te bevoordelen:

```
asa# sh run all crypto engine
crypto engine accelerator-bias ssl
asa# show crypto accelerator load-balance

[..]
                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions            Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 7      Total: 166714  Active:   205         100.0%
[..]
```

De actieve Session Distribution zal altijd 100% zijn, ongeacht het huidige crypto-gebruik van het platform.

Opmerking: De volgende platforms zijn beschikbaar voor een nieuw evenwicht in cryptografische core: ASA 5585, 5580, 5545/555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 en ASM.

FAQ

Licentie

V: Waarom kan ik geen AnyConnect-software downloaden?

A: U moet de AnyConnect Plus- of Apex-licentie aanschaffen om de AnyConnect-client te kunnen downloaden. Daarna zou je recht moeten hebben. Als u geen recht hebt ondanks het aanschaffen van de AnyConnect Apex of Plus-licentie, opent u een case met rechten om dit probleem op te lossen.

V: Waarom zie ik 9999 aangeschaft voor de AnyConnect-licentie in mijn slimme licentiekaart?

A: Dit wordt verwacht met bepaalde AnyConnect-licenties, zoals de AnyConnect Plus onbeperkt of niet-verbonden AnyConnect Plus- of Apex-licenties.

V: Wat bepaalt wanneer "In gebruik" stappen?

A: Deze waarde vermindert wanneer een apparaat dat de AnyConnect-licentie gebruikt, wordt geregistreerd. Als u FMC bijvoorbeeld registreert, voegt u de AnyConnect Plus-licentie toe aan een apparaat, dan wordt de waarde in gebruik voor de AnyConnect Plus-licentie bepaald. Deze waarde is **NIET** gebaseerd op huidige gebruikerssessies. Het registreren van ASAv-apparaten verlaagt **NIET** de "In-use"-telling. Dit is een bekende cosmetische kwestie. U kunt niet meer apparaten registreren dan het aantal geautoriseerde gebruikers dat is aangeschaft.

V: Wat bepaalt de gekochte waarde?

A: De aankoopwaarde wordt bepaald door het aantal geautoriseerde gebruikers dat bij de licentie is aangeschaft. Een AnyConnect Plus-licentie van 25 gebruikers heeft bijvoorbeeld een aangeschafte telling.

V: Hoe kan ik een sterke encryptie mogelijk maken?

A: Om sterke encryptie mogelijk te maken, moet u het vakje "Laat export-gecontroleerd functionaliteit op de producten toestaan die met deze token geregistreerd zijn" aankruisen wanneer u het registrtoken maakt.

V: Hoe converteer ik van PAK naar slimme licenties?

A: U dient hiervoor een case te openen met Licentie.

V: Als ik een X-gebruikerslicentie heb, wat gebeurt er dan als "X+1" of meer gebruikers verbinding maken met het apparaat?

A: Met de Apex- en Plus-licentie wordt de volledige VPN-gebruikerscapaciteit van het apparaat ontgrendeld. Zolang het apparaat niet zijn maximale VPN-gebruikerslimiet bereikt, blijft het apparaat verbindingen accepteren. Er is geen handhaving op het apparaat voor VPN-gebruikerssessies en het is op basis van eer. Het is uw verantwoordelijkheid om extra geautoriseerde gebruikerslicenties te kopen als het gebruik van de VPN-sessie voor het apparaat moet worden verhoogd. Om het maximum aantal gebruikers te controleren dat door het apparaat wordt ondersteund, controleert u het gegevensblad voor het apparaat op de website van Cisco of ***laat u VPN-sessiondb*** uitvoeren en onderzoekt u de "Devices Total VPN Capacity". Voor ASA's, kunt u de ***show versie*** ook uitvoeren of de opdrachten ***voor de samenvatting*** van de ***vpn-sessiondb*** laten ***zien***.

V: Hoe kan ik controleren of de licentie op mijn apparaat is geactiveerd?

A: Op FTD's kunt u geen AnyConnect-configuratie implementeren tenzij de licentie is geactiveerd. Op ASA's, kunt u de ***show versie*** controleren of de ***vpn-sessiesamenvatting van de show laten zien*** om te onderzoeken hoeveel gebruikers zijn toegestaan. Zonder een actieve licentie zijn er maximaal 2 gebruikers. Opmerking over de ASA, de bovengenoemde opdrachten zullen de Plus/Apex-licentieinformatie niet weergeven. Dit wordt gevolgd door het verbeteringsverzoek CSCuw74731.

Configuratie

V: Welke ASA-platforms kan ik gebruiken voor het in evenwicht brengen van VPN-belasting? Kan ik verschillende ASA-hardwareplatforms of verschillende software versies in een VPN-taakverdeling-cluster gebruiken?

A: Ja, een VPN-taakverdeling kan bestaan uit verschillende fysieke of virtuele ASA-modellen, inclusief de ASAv. In het algemeen wordt echter aanbevolen dat het cluster homogeen is. Als verschillende softwareversies worden gebruikt in een vpn-load-balanceercluster, worden alleen IPsec-sessies ondersteund. Raadpleeg voor meer informatie: Richtsnoeren en Beperkingen voor VPN-taakverdeling.

V: Hoe stel ik een split-tunneling in? Kan je bepaalde soorten toepassingsverkeer, zoals Office 365, uitsluiten van een tunnelconfiguratie?

A: Zie Cisco Community-artikel AnyConnect Split-tunneling voor configuratievoorbeelden van verschillende gebruiksgevallen. U kunt ook een combinatie van gesplitste tunneling en dynamische gespleten tunneling gebruiken om op toepassing gebaseerde gesplitste tunneling te bereiken. Bij een voorbeeld hoe u AnyConnect-splitsingen voor Office 365 en Webex kunt optimaliseren, zie Hoe u AnyConnect kunt optimaliseren voor de verbindingen van Microsoft Office365 en Cisco Webex.

V: Ik zie de fout "Onvertrouwde certificeringswaarschuwing" bij verbinding met een ASA-head-end met AnyConnect. Waarom gebeurt dit?

A: Dit is waarschijnlijk omdat de head-end een zelfgetekend certificaat gebruikt. Om dit te repareren, kan een SSL-certificaat worden aangeschaft bij een certificaatinstantie en op het hoofd van de ASA worden geïnstalleerd. Raadpleeg voor gedetailleerde implementatiestappen: ASA configureren: SSL digitale certificaatinstallatie en -vernieuwing.

V: Worden wildkaartcertificaten ondersteund op Cisco RAVPN-kopeinden?

A: Ja, jokerteken en certificaten met DNS onderwerp alternatieve namen (SAN's) worden ondersteund.

V: Kan één apparaat zowel taakverdeling als failover gebruiken?

A: Active/stand-by failover wordt ondersteund met VPN-taakverdeling. Het standby apparaat zal onmiddellijk overnemen zonder dat dit van invloed is op de VPN-tunnel als de actieve eenheid defect is. VPN-taakverdeling wordt niet ondersteund met een actieve/actieve failover-configuratie.

Controleren

Vraag: Welke SNMP MIB kan ik gebruiken om het ASA CPU-gebruik te controleren?

A: CISCO-PROCESS-MIB kan worden gebruikt om het ASA CPU-gebruik te bewaken. Raadpleeg voor een volledige lijst met ondersteunde MIB's: Adaptieve security applicatie MIB Support List. Ook om een lijst van de ondersteunde SNMP MIBs en OIDs voor een specifieke ASA te verkrijgen kan men de volgende opdracht uitgeven: ***toon een server-oidlist.***

V: Hoe controleer ik het aantal gebruikers dat momenteel op een VPN-head-end is aangesloten?

A: Gebruik ***show vpn-sessiondb*** van de CLI om het huidige aantal gebruikers op een ASA of FTD of SNMP MIB te controleren

CISCO-REMOTE-ACCESS-MONITOR-MIB.

Probleemoplossing

V: Sommige van onze AnyConnect VPN-gebruikers lijken regelmatig verbindingen te ervaren. Hoe kan ik dergelijke problemen oplossen:

A: Raadpleeg voor het oplossen van VPN-problemen en andere gebruikelijke AnyConnect-problemen het volgende: AnyConnect VPN-clientprobleemoplossing - Gemeenschappelijke problemen.

V: Wanneer een bepaalde hoeveelheid gebruikers verbinding maakt met het VPN-head-end, kunnen geen gebruikers meer verbinding maken. De licentie is op het apparaat geactiveerd en ***toont VPN-sessiondb*** aan dat het apparaat meer gebruikers kan verwerken. Wat zou het probleem kunnen zijn?

A: Controleer de VPN-adrespool voor deze gebruikers om er zeker van te zijn dat het aantal gebruikers dat een verbinding maakt, niet groter is dan de hoeveelheid adressen die beschikbaar zijn. U kunt verifiëren met de opdracht ***ip lokale pool [poolnaam]***. Een andere potentiele oorzaak op oudere platforms is dat de ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit opdracht*** is ingesteld op een lage waarde. U kunt dit verifiëren met de opdracht ***show run alle vpn-sessiondb***. Als dit zich voordoet, kan de waarde worden verhoogd of kan de opdracht worden verwijderd om deze limiet te voorkomen.

Extra help verkrijgen

Neem voor extra assistentie contact op met TAC. Een geldig ondersteuningscontract is vereist: Cisco's wereldwijde contactgegevens voor ondersteuning

U kunt hier ook de Cisco VPN-community bezoeken.

Daarnaast kunt u de TAC Security Show Podcasts controleren

Referenties

Hieronder vindt u aanvullende links naar andere bronnen die nuttig zijn voor AnyConnect-implementaties en de behandeling van COVOD-19-gerelateerde kwesties in het algemeen.

- Cisco Security reageert op een toename in aantal externe werknemers - Cisco Community
- AnyConnect-bestelgids
- AnyConnect-licenties
- AnyConnect VPN, ASA en FTD FAQ voor beveiligde externe werknemers